Journal of Number Theory 133 (2013) 719–737

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the Diophantine equation $n^2 = x^2 + by^2 + cz^2$

Shaun Cooper *, Heung Yeung Lam

Institute of Information and Mathematical Sciences, Massey University-Albany, Private Bag 102904, North Shore Mail Centre, Auckland, New Zealand

ARTICLE INFO

Article history:
Received 2 May 2011
Accepted 29 August 2012
Available online 30 October 2012
Communicated by David Goss

MSC:
primary 11E25
secondary 11F11

Keywords:
Sum of five squares
Theta function

ABSTRACT

For any positive integer n we state and prove formulas for the number of solutions, in integers, of $n^2 = x^2 + y^2 + 2z^2$, $n^2 = x^2 + 2y^2 + 2z^2$, $n^2 = x^2 + y^2 + 3z^2$ and $n^2 = x^2 + 3y^2 + 3z^2$. Some conjectures are listed at the end of the paper.

1. Introduction

Let n be any positive integer and denote its prime factorization by

$$n = 2^{\lambda_2} \prod_p p^{\lambda_p}. \tag{1}$$

Here and throughout this work the symbol $\prod_p$ will denote a product over odd primes p, and any empty product is defined to be 1. More than one hundred years ago, A. Hurwitz [11] noted

Theorem 1.1. *The number of* $(x, y, z) \in \mathbf{Z}^3$ *such that*

$$n^2 = x^2 + y^2 + z^2$$

* Corresponding author.
E-mail addresses: s.cooper@massey.ac.nz (S. Cooper), h.y.lam@massey.ac.nz (H.Y. Lam).

http://dx.doi.org/10.1016/j.jnt.2012.08.020

is given by

$$6\prod_p\left[\frac{p^{\lambda_p+1}-1}{p-1}-\left(\frac{-1}{p}\right)\frac{p^{\lambda_p}-1}{p-1}\right], \tag{2}$$

where the values of the Legendre symbol are given by

$$\left(\frac{-1}{p}\right)=\begin{cases}1 & \text{if } p\equiv 1 \pmod 4,\\ -1 & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

Hurwitz indicated that Theorem 1.1 could be proved using the techniques of his paper [10]. A complete proof of Theorem 1.1 using Hurwitz's technique has been given by C.D. Olds [12]. The first goal of this work is to establish the following analogues of Theorem 1.1 for each of the quadratic forms $x^2+y^2+2z^2$ and $x^2+y^2+3z^2$:

Theorem 1.2. *The number of* $(x,y,z)\in\mathbf{Z}^3$ *such that*

$$n^2=x^2+y^2+2z^2$$

is given by

$$4b(\lambda_2)\prod_p\left[\frac{p^{\lambda_p+1}-1}{p-1}-\left(\frac{-2}{p}\right)\frac{p^{\lambda_p}-1}{p-1}\right], \tag{3}$$

where

$$b(\lambda_2)=\begin{cases}1 & \text{if } \lambda_2=0,\\ 3 & \text{if } \lambda_2\geqslant 1,\end{cases}$$

and the values of the Legendre symbol are given by

$$\left(\frac{-2}{p}\right)=\begin{cases}1 & \text{if } p\equiv 1 \text{ or } 3 \pmod 8,\\ -1 & \text{if } p\equiv 5 \text{ or } 7 \pmod 8.\end{cases}$$

Theorem 1.3. *The number of* $(x,y,z)\in\mathbf{Z}^3$ *such that*

$$n^2=x^2+y^2+3z^2$$

is given by

$$4\left(2^{\lambda_2+1}-1\right)\prod_{p\geqslant 5}\left[\frac{p^{\lambda_p+1}-1}{p-1}-\left(\frac{-3}{p}\right)\frac{p^{\lambda_p}-1}{p-1}\right], \tag{4}$$

where the values of the Legendre symbol are given by

$$\left(\frac{-3}{p}\right)=\begin{cases}1 & \text{if } p\equiv 1 \pmod 6,\\ -1 & \text{if } p\equiv 5 \pmod 6.\end{cases}$$

Theorems 1.2 and 1.3 generalize recent work of B. Cho, D. Kim and J.K. Koo [4]. They proved that for an odd prime p, the number of $(x, y, z) \in \mathbf{Z}^3$ such that $p^2 = x^2 + y^2 + 2z^2$ or $p^2 = x^2 + y^2 + 3z^2$ is given by $4(p + 1 - (\frac{-2}{p}))$ or $4(p + 1 - (\frac{-3}{p}))$, respectively. The latter result had been conjectured earlier by Z.H. Sun [15, Conjecture 17], and holds for primes $p \geqslant 5$. The results of Cho et al. are the special cases of Theorems 1.2 and 1.3 for which n is an odd prime (and the prime is at least 5 in the latter case).

We will also prove analogues of Theorems 1.1–1.3 for the quadratic forms $x^2 + 2y^2 + 2z^2$ and $x^2 + 3y^2 + 3z^2$:

Theorem 1.4. *The number of* $(x, y, z) \in \mathbf{Z}^3$ *such that*

$$n^2 = x^2 + 2y^2 + 2z^2$$

is given by

$$2b(\lambda_2) \prod_p \left[\frac{p^{\lambda_p+1} - 1}{p - 1} - \left(\frac{-1}{p} \right) \frac{p^{\lambda_p} - 1}{p - 1} \right],$$

where the value of $b(\lambda_2)$ *is the same as for Theorem* 1.2.

Theorem 1.5. *The number of* $(x, y, z) \in \mathbf{Z}^3$ *such that*

$$n^2 = x^2 + 3y^2 + 3z^2$$

is given by

$$2\left(2^{\lambda_2+2} - 3\right) \prod_{p \geqslant 5} \left[\frac{p^{\lambda_p+1} - 1}{p - 1} - \left(\frac{-1}{p} \right) \frac{p^{\lambda_p} - 1}{p - 1} \right].$$

This work is organized as follows. In Section 2 we will describe Hurwitz's technique as elucidated by H.F. Sandham [14]. Section 3 contains a proof of Theorem 1.2. The proof of Theorem 1.3 is more difficult and is given in Sections 4 and 5. The prime 2 requires special treatment, and this is handled in Section 4. Section 5 contains the analysis for the odd primes. Theorem 1.4 is deduced from Hurwitz's Theorem 1.1 in Section 6. Theorem 1.5 is proved in Section 7. Some conjectures and scope for future work are detailed in Section 8.

2. Hurwitz's technique

In this section we establish some notation that will be used throughout, and state Hurwitz's technique.

Let $c_1, c_2, \ldots, c_\ell$ be positive integers. Let $r_{(c_1,c_2,\ldots,c_\ell)}(m)$ denote the number of $(x_1, x_2, \ldots, x_\ell) \in \mathbf{Z}^\ell$ such that

$$m = c_1 x_1^2 + c_2 x_2^2 + \cdots + c_\ell x_\ell^2.$$

For example, the values of $r_{(1,1,1)}(n^2)$, $r_{(1,1,2)}(n^2)$ and $r_{(1,1,3)}(n^2)$ are given by (2), (3) and (4), respectively. For any positive numbers $c_1, c_2, \ldots, c_\ell$,

$$r_{(c_1,c_2,\ldots,c_\ell)}(0) = 1.$$

Ramanujan's theta functions $\varphi(q)$ and $\psi(q)$ are defined by

$$\varphi(q)=\sum_{j=-\infty}^{\infty} q^{j^2} \quad \text{and} \quad \psi(q)=\sum_{j=0}^{\infty} q^{j(j+1)/2}. \tag{5}$$

Clearly,

$$\sum_{m=0}^{\infty} r_{(c_1,c_2,\ldots,c_\ell)}(m)q^m=\varphi\big(q^{c_1}\big)\varphi\big(q^{c_2}\big)\cdots\varphi\big(q^{c_\ell}\big).$$

For future reference, we record the result [1, p. 40]:

$$\varphi(q)\psi\big(q^2\big)=\psi^2(q). \tag{6}$$

For any positive integer n, the sum of divisors function $\sigma(n)$ is defined by

$$\sigma(n)=\sum_{d|n} d,$$

and the Möbius function $\mu(n)$ is defined by

$$\mu(n)=\begin{cases} 1 & \text{if } n=1,\\ 0 & \text{if } n \text{ is divisible by the square of some prime},\\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes}.\end{cases}$$

We now describe Hurwitz's technique, as summarized by Sandham [14].

Lemma 2.1. *Suppose that $N(n)$ is a function, defined for all non-negative integers n, that satisfies the property*

$$N(pn)=N(p)N(n)-f(p)N\left(\frac{n}{p}\right) \tag{7}$$

for all primes p, where f is a completely multiplicative function. Then the coefficient of q^{n^2} in

$$\left(\sum_{j=-\infty}^{\infty} q^{j^2}\right)\times\left(\sum_{k=0}^{\infty} N(k)q^k\right)$$

is equal to

$$\sum_{r=1}^{\infty} M\left(\frac{2n}{r}\right) f(r)\mu(r)$$

where

$$\sum_{n=0}^{\infty} M(n)q^n=\left(\sum_{k=0}^{\infty} N(k)q^k\right)^2,$$

and $M(x)$ is defined to be 0 if x is not a non-negative integer.

Proof. See [14, Section 2]. □

Note that in order for the condition (7) to be satisfied when $n=0$, we must either have $N(0)=0$ or $N(p)=1+f(p)$ for all primes p.

3. Proof of Theorem 1.2

Recall that the values of the Jacobi symbol with numerator -2 are given by

$$\left(\frac{-2}{n}\right)=\begin{cases}1 & \text{if } n\equiv 1 \text{ or } 3 \pmod 8,\\ -1 & \text{if } n\equiv 5 \text{ or } 7 \pmod 8,\\ 0 & \text{otherwise.}\end{cases}$$

The Jacobi symbol with numerator -2 is a completely multiplicative function, that is,

$$\left(\frac{-2}{mn}\right)=\left(\frac{-2}{m}\right)\left(\frac{-2}{n}\right)$$

for all positive integers m and n.

The next lemma is fundamental to our proof.

Lemma 3.1. *Let n be a positive integer and let its prime factorization be given by (1). The number of $(x,y)\in\mathbf{Z}^2$ such that*

$$n=x^2+2y^2$$

is given by

$$r_{(1,2)}(n)=2\sum_{d\mid n}\left(\frac{-2}{d}\right)=2\prod_{(\frac{-2}{p})=1}(\lambda_p+1)\prod_{(\frac{-2}{p})=-1}\frac{1+(-1)^{\lambda_p}}{2}. \tag{8}$$

The number of $(x,y,z,w)\in\mathbf{Z}^4$ such that

$$n=x^2+y^2+2z^2+2w^2$$

is given by

$$\begin{aligned} r_{(1,1,2,2)}(n)&=4\sigma(n)-4\sigma\left(\frac{n}{2}\right)+8\sigma\left(\frac{n}{4}\right)-32\sigma\left(\frac{n}{8}\right)\\ &=4c(\lambda_2)\prod_p\frac{p^{\lambda_p+1}-1}{p-1} \end{aligned}\tag{9}$$

where

$$c(\lambda_2)=\begin{cases}1 & \text{if } \lambda_2=0,\\ 2 & \text{if } \lambda_2=1,\\ 6 & \text{if } \lambda_2\geqslant 2.\end{cases}$$

Proof. See [3, pp. 74, 83], [7, (31.12)] and [8] for proofs of the first equality in (8) and for references; this result was known to Dirichlet. The second equality in (8) follows by expressing the divisors of n in terms of the prime factors and noting that the resulting sum splits into a multiple sum, one sum for each distinct prime factor of n. Each single sum can then be summed independently.

Proofs of the first equality in (9) can be found in [7, (31.32)] or [16, p. 267], and a proof of an equivalent result, in terms of the generating function, is in [2, p. 373]. References to other proofs are given in [16, p. 278]. The second equality follows by expressing the divisors of n in terms of the prime factors. $\square$

We are now ready for

Proof of Theorem 1.2. For any non-negative integer n, define $N(n)$ and $M(n)$ by

$$N(n) = \frac{1}{2} r_{(1,2)}(n) \quad \text{and} \quad M(n) = \frac{1}{4} r_{(1,1,2,2)}(n), \tag{10}$$

and note that

$$\sum_{n=0}^{\infty} M(n) q^n = \left(\sum_{n=0}^{\infty} N(n) q^n \right)^2 .$$

We define $M(x) = 0$ if x is not a non-negative integer. By (8) we deduce that for all positive integers n and all primes p, we have

$$N(pn) = N(p)N(n) - \left(\frac{-2}{p}\right) N\left(\frac{n}{p}\right)$$

and

$$N(p) = 1 + \left(\frac{-2}{p}\right).$$

Thus, the condition (7) in Lemma 2.1 holds for the completely multiplicative function given by $f(n) = (\frac{-2}{n})$.

Let n be any positive integer and let its prime factorization be given by (1). Then,

$$\begin{aligned} r_{(1,1,2)}(n^2) &= \text{coefficient of } q^{n^2} \text{ in } \left(\sum_{j=-\infty}^{\infty} q^{j^2} \right) \times \left(\sum_{k,\ell=-\infty}^{\infty} q^{k^2+2\ell^2} \right) \\ &= 2 \times \text{coefficient of } q^{n^2} \text{ in } \left(\sum_{j=-\infty}^{\infty} q^{j^2} \right) \times \left(\sum_{k=0}^{\infty} N(k) q^k \right). \end{aligned}$$

By Lemma 2.1, this simplifies to

$$r_{(1,1,2)}(n^2) = 2 \sum_{r=1}^{\infty} M\left(\frac{2n}{r}\right) \left(\frac{-2}{r}\right) \mu(r).$$

By (9) and (10), this can be expressed in terms of the prime factors of n to give

$$\begin{aligned} r_{(1,1,2)}\left(n^2\right) &= 2M(2n)\prod_p\left(1-\left(\frac{-2}{p}\right)\frac{M(\frac{2n}{p})}{M(2n)}\right) \\ &= 2c(\lambda_2+1)\prod_p\frac{p^{\lambda_p+1}-1}{p-1}\prod_p\left(1-\left(\frac{-2}{p}\right)\frac{p^{\lambda_p}-1}{p^{\lambda_p+1}-1}\right) \\ &= 2c(\lambda_2+1)\prod_p\left(\frac{p^{\lambda_p+1}-1}{p-1}-\left(\frac{-2}{p}\right)\frac{p^{\lambda_p}-1}{p-1}\right). \end{aligned}$$

On using the value of $c(\lambda_2)$ given by Lemma 3.1, we complete the proof of Theorem 1.2. □

4. Proof of Theorem 1.3: Part 1

It is natural to try to tweak the proof of Theorem 1.2 by replacing the functions $N(n)$ and $M(n)$ in (10) with

$$N(n)=\frac{1}{2}r_{(1,3)}(n) \quad \text{and} \quad M(n)=\frac{1}{4}r_{(1,1,3,3)}(n), \tag{11}$$

respectively. By a classical result of L. Lorenz (see [3, pp. 75, 83], [7, (31.17), (31.18)] and [8] for proofs and references) we have

$$\begin{aligned} r_{(1,3)}(n) &= 2\sum_{d\mid n}\left(\frac{-3}{d}\right)+4\sum_{d\mid \frac{n}{4}}\left(\frac{-3}{d}\right) \\ &= 2d(\lambda_2)\prod_{p\equiv 1 \pmod 6}(\lambda_p+1)\prod_{p\equiv 5 \pmod 6}\frac{1+(-1)^{\lambda_p}}{2} \end{aligned}$$

where

$$d(\lambda_2)=\begin{cases} 1 & \text{if } \lambda_2=0, \\ 0 & \text{if } \lambda_2 \text{ is odd}, \\ 3 & \text{if } \lambda_2>0 \text{ and } \lambda_2 \text{ is even}, \end{cases}$$

and the values of the Jacobi symbol with numerator -3 are given by

$$\left(\frac{-3}{n}\right)=\begin{cases} 1 & \text{if } n\equiv 1 \pmod 3, \\ -1 & \text{if } n\equiv 2 \pmod 3, \\ 0 & \text{otherwise}. \end{cases}$$

It follows that the function $N(n)$ given by (11) does not satisfy the hypothesis (7) in Hurwitz's technique for the prime $p=2$. A modification of the technique is required, and we shall accomplish this in two steps. First of all, in this section we will prove:

Proposition 4.1. *Let m be a positive odd integer and let λ be a non-negative integer. Then*

$$r_{(1,1,3)}\left(2^{2\lambda}m^2\right)=\left(2^{\lambda+1}-1\right)r_{(1,1,3)}\left(m^2\right).$$

Second, in the next section we will determine the value of $r_{(1,1,3)}(m^2)$ for odd values of m. This will complete the proof of Theorem 1.3.

The remainder of this section is devoted to proving Proposition 4.1. We will require the following three lemmas.

Lemma 4.2. *Let $\varphi(q)$ and $\psi(q)$ be Ramanujan's theta functions defined by (5). The following dissections into even and odd parts hold*:

$$\varphi(q)=\varphi\left(q^4\right)+2q\psi\left(q^8\right),$$
$$\varphi^2(q)=\varphi^2\left(q^2\right)+4q\psi^2\left(q^4\right),$$
$$\psi^2(q)=\varphi\left(q^4\right)\psi\left(q^2\right)+2q\psi\left(q^2\right)\psi\left(q^8\right),$$
$$\psi(q)\psi\left(q^3\right)=\varphi\left(q^6\right)\psi\left(q^4\right)+q\varphi\left(q^2\right)\psi\left(q^{12}\right).$$

Proof. These are (i), (ii), (xiii) and (xxxiii), respectively, in [5]. □

In order to state the next lemma, it will be convenient to introduce the slash operator. Let $f(q)$ have a q-expansion given by

$$f(q)=\sum_{j=0}^{\infty}c_jq^j,$$

and let m be a positive integer. The slash operator $f(q)|_m$ is defined by

$$f(q)|_m=\sum_{j=0}^{\infty}c_jq^j\Big|_m=\sum_{j=0}^{\infty}c_{mj}q^j.$$

Clearly, for any positive integers m and n, we have

$$\left(\sum_{j=0}^{\infty}c_jq^j|_m\right)\Bigg|_n=\sum_{j=0}^{\infty}c_jq^j|_{mn}.$$

Lemma 4.3. *The following identities hold*:

$$\varphi^2(q)\varphi\left(q^3\right)\big|_4=\varphi^2(q)\varphi\left(q^3\right)+8q\psi^2(q)\psi\left(q^6\right),\tag{12}$$
$$q\psi^2(q)\psi\left(q^6\right)\big|_4=2q\psi^2(q)\psi\left(q^6\right),\tag{13}$$

and

$$\varphi^2(q)\varphi\left(q^3\right)\big|_{16}=3\varphi^2(q)\varphi\left(q^3\right)\big|_4-2\varphi^2(q)\varphi\left(q^3\right).\tag{14}$$

Proof. By Lemma 4.2 we have

$$\varphi^2(q)\varphi\left(q^3\right)=\left(\varphi\left(q^4\right)+2q\psi\left(q^8\right)\right)^2\left(\varphi\left(q^{12}\right)+2q^3\psi\left(q^{24}\right)\right).$$

If we expand the right hand side, and group the terms according to the powers modulo 4, we get

$$\begin{aligned}\varphi^2(q)\varphi(q^3) = {} & \big(\varphi^2(q^4)\varphi(q^{12}) + 8q^4\varphi(q^4)\psi(q^8)\psi(q^{24})\big) \\ & + 4q\big(\varphi(q^4)\varphi(q^{12})\psi(q^8) + 2q^4\psi^2(q^8)\psi(q^{24})\big) \\ & + 4q^2\psi^2(q^8)\varphi(q^{12}) + 2q^3\varphi^2(q^4)\psi(q^{24}).\end{aligned} \tag{15}$$

Now extract the powers that are congruent to 0 (mod 4), apply (6), and then replace q^4 with q; the result is (12).

Next, by Lemma 4.2 again, we have

$$q\psi^2(q)\psi(q^6) = q\varphi(q^4)\psi(q^2)\psi(q^6) + 2q^2\psi(q^2)\psi(q^6)\psi(q^8).$$

Extract the terms that involve even powers of q, then replace q^2 with q, to get

$$q\psi^2(q)\psi(q^6)\big|_2 = 2q\psi(q)\psi(q^3)\psi(q^4).$$

Apply Lemma 4.2 to the right hand side, to get

$$q\psi^2(q)\psi(q^6)\big|_2 = 2q\varphi(q^6)\psi^2(q^4) + 2q^2\varphi(q^2)\psi(q^4)\psi(q^{12}).$$

If we extract the terms that involve even powers of q, apply (6), and then replace q^2 with q, the result is (13).

Finally, the identity (14) follows by applying the $|_4$ operator to the identity (12), and making use of (13). $\square$

Lemma 4.4. *The following identities hold*:

$$\sum_{n=0}^{\infty} r_{(1,1,3)}(4n+1)q^n = 4\psi^2(q)\varphi(q^3) + 8q\psi^2(q^2)\psi(q^6)$$

and

$$\sum_{n=0}^{\infty} r_{(1,1,3)}(16n+4)q^n = 12\psi^2(q)\varphi(q^3) + 8q\psi^2(q^2)\psi(q^6).$$

Proof. The first result follows from (15) by extracting the powers that are congruent to 1 (mod 4), and then applying (6). The second result follows by starting with (12) and then using Lemma 4.2 to extract the powers that are congruent to 1 (mod 4). The procedure is similar to the proof of Lemma 4.3, so we omit the details. $\square$

We are now ready for

Proof of Proposition 4.1. We fix a positive odd integer m, and let

$$f(\lambda) = r_{(1,1,3)}(2^{2\lambda}m^2).$$

By (14) we have

$$f(\lambda) = 3f(\lambda - 1) - 2f(\lambda - 2) \tag{16}$$

provided λ is an integer and $\lambda \geqslant 2$.

If we compare even powers of q in the identities in Lemma 4.4, we deduce that

$$r_{(1,1,3)}(32n + 4) = 3r_{(1,1,3)}(8n + 1),$$

that is,

$$r_{(1,1,3)}(4n) = 3r_{(1,1,3)}(n) \quad \text{if } n \equiv 1 \pmod 8. \tag{17}$$

As m is odd and consequently $m^2 \equiv 1 \pmod 8$, on taking $n = m^2$ in (17) we deduce that

$$f(1) = 3f(0). \tag{18}$$

The solution of the linear recurrence relation (16), with initial conditions given by (18) and

$$f(0) = r_{(1,1,3)}\big(m^2\big),$$

is $f(\lambda) = (2^{\lambda+1} - 1)r_{(1,1,3)}(m^2)$. This completes the proof of Proposition 4.1. $\square$

5. Proof of Theorem 1.3: Part 2

In this section, we will work with the character modulo 6 defined on the integers by

$$\chi(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 6, \\ -1 & \text{if } n \equiv 5 \pmod 6, \\ 0 & \text{otherwise.} \end{cases} \tag{19}$$

We note that

$$\chi(p) = \left(\frac{-3}{p}\right) \quad \text{for all primes } p \neq 2. \tag{20}$$

The goal of this section is to prove

Proposition 5.1. *Let m be a positive odd number, and let its prime factorization be given by $m = \prod_p p^{\lambda_p}$, where the product is over odd primes p. Then*

$$r_{(1,1,3)}\big(m^2\big) = 4\prod_{p \geqslant 5}\left[\frac{p^{\lambda_p+1} - 1}{p - 1} - \chi(p)\frac{p^{\lambda_p} - 1}{p - 1}\right].$$

Note that neither the prime $p = 3$ nor its exponent λ_3 appear in this formula for $r_{(1,1,3)}(m^2)$. In view of (20), Propositions 4.1 and 5.1 immediately imply Theorem 1.3.

In order to prove Proposition 5.1 we will require the following two lemmas.

Lemma 5.2. *For Ramanujan's theta functions $\varphi(q)$ and $\psi(q)$ defined by (5), and for the character $\chi(n)$ defined by (19), the following identities hold:*

$$q\psi(q^2)\psi(q^6) = \sum_{n=1}^{\infty} \frac{\chi(n)q^n}{1-q^{2n}}, \tag{21}$$

$$q\psi^2(q)\psi^2(q^3) = \sum_{\substack{n=1 \\ 3\nmid n}}^{\infty} \frac{nq^n}{1-q^{2n}}, \tag{22}$$

and

$$\varphi(q)\varphi(q^3) - \varphi(-q)\varphi(-q^3) = 4q\psi(q^2)\psi(q^6). \tag{23}$$

Proof. The first two results were listed by Ramanujan in his second notebook [13, Chapter 19, Entry 3]. See [1, pp. 223–225] or [7, (32.27), (33.2)] for proofs. The last result is equivalent to the modular equation of degree 3. There are many proofs of this result, for example, see [1, p. 232], [3, p. 145], [6] or [7, (34.8)]. □

Lemma 5.3. *Let n be a positive integer with prime factorization given by (1). Let $N(n)$ and $M(n)$ be defined by*

$$N(n) = \begin{cases} \frac{1}{2}r_{(1,3)}(n) & \text{if } n \text{ is odd}, \\ 0 & \text{if } n \text{ is even}, \end{cases}$$

and

$$\sum_{n=1}^{\infty} M(n)q^n = \left(\sum_{n=1}^{\infty} N(n)q^n\right)^2.$$

For any real number x, define $N(x) = M(x) = 0$ if x is not a positive integer. Then,

$$N(n) = \begin{cases} \prod_{\chi(p)=1}(1+\lambda_p)\prod_{\chi(p)=-1}(\frac{1+(-1)^{\lambda_p}}{2}) & \text{if } n \text{ is odd}, \\ 0 & \text{if } n \text{ is even}, \end{cases} \tag{24}$$

and

$$M(2n) = 2^{\lambda_2}\prod_{p\geqslant 5}\frac{p^{\lambda_p+1}-1}{p-1}. \tag{25}$$

Proof. By the definitions of $N(n)$ and $\varphi(q)$, we have

$$\sum_{n=1}^{\infty} N(n)q^n = \frac{1}{2}\sum_{n=0}^{\infty} r_{(1,3)}(2n+1)q^{2n+1} = \frac{1}{4}\big(\varphi(q)\varphi(q^3) - \varphi(-q)\varphi(-q^3)\big).$$

Now apply Lemma 5.2 to get

$$\sum_{n=1}^{\infty} N(n)q^n = q\psi(q^2)\psi(q^6) = \sum_{n=1}^{\infty} \frac{\chi(n)q^n}{1-q^{2n}}. \tag{26}$$

If we expand in powers of q and equate coefficients of q^n, we get

$$N(n) = \begin{cases} \sum_{d|n} \chi(d) & \text{if } n \text{ is odd,} \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

Now express each divisor d in terms of the prime factors of n to obtain (24).

Next, by the definition of $M(n)$, (22) and (26), we have

$$\sum_{n=1}^{\infty} M(n)q^n = \left(\sum_{n=1}^{\infty} N(n)q^n\right)^2 = q^2\psi^2(q^2)\psi^2(q^6) = \sum_{\substack{j=1 \\ 3\nmid j}}^{\infty} \frac{jq^{2j}}{1-q^{4j}}.$$

Therefore,

$$M(2n) = \text{coefficient of } q^n \text{ in } \sum_{\substack{j=1 \\ 3\nmid j}}^{\infty} \sum_{k=1}^{\infty} jq^{j(2k-1)} = \sum_{\substack{d|n, 3\nmid d \\ n/d \text{ odd}}} d.$$

Now express each divisor d in terms of the prime factors of n to obtain (25). $\square$

We are now ready for

Proof of Proposition 5.1. Since m is odd, the only solutions of $j^2+k^2+3\ell^2 = m^2$ occur when exactly one of j and k is even. Therefore,

$$\begin{aligned} r_{(1,1,3)}(m^2) &= 2 \times \text{number of solutions of } \{j^2+k^2+3\ell^2 = m^2,\ j \text{ even}\} \\ &= 2\sum_{j \text{ even}} r_{(1,3)}(m^2-j^2) \\ &= 4\sum_{j \text{ even}} N(m^2-j^2) \\ &= 4\sum_{j=-\infty}^{\infty} N(m^2-j^2), \end{aligned}$$

where the last step holds because the additional terms are all zero. Therefore,

$$r_{(1,1,3)}(m^2) = 4 \times \text{coefficient of } q^{m^2} \text{ in } \left(\sum_{j=-\infty}^{\infty} q^{j^2}\right)\left(\sum_{n=0}^{\infty} N(n)q^n\right).$$

The identity (24) may be used to verify that $N(n)$ satisfies the hypothesis (7) in Hurwitz's technique for all primes p, where $f(p) = \chi(p)$. Moreover, $N(0) = 0$. Therefore, by Lemma 2.1, we obtain

$$r_{(1,1,3)}(m^2) = 4\sum_{r=1}^{\infty} M\left(\frac{2m}{r}\right)\chi(r)\mu(r).$$

Since m is odd, by (25) we get

$$\begin{aligned} r_{(1,1,3)}\left(m^2\right) &= 4M(2m)\prod_{p\geqslant 5}\left(1-\chi(p)\frac{M(\frac{2m}{p})}{M(2m)}\right) \\ &= 4\prod_{p\geqslant 5}\frac{p^{\lambda_p+1}-1}{p-1}\prod_{p\geqslant 5}\left(1-\chi(p)\frac{p^{\lambda_p}-1}{p-1}\right) \\ &= 4\prod_{p\geqslant 5}\left[\frac{p^{\lambda_p+1}-1}{p-1}-\chi(p)\frac{p^{\lambda_p}-1}{p-1}\right]. \end{aligned}$$

This completes the proof of Proposition 5.1. □

6. Proof of Theorem 1.4

Of all of Theorems 1.2–1.5, Theorem 1.4 is the easiest to prove because it can be deduced from Hurwitz's Theorem 1.1. Here is the proof.

Proof of Theorem 1.4. By the first two parts of Lemma 4.2, we have

$$\varphi(q)\varphi^2\left(q^2\right)=\left(\varphi\left(q^4\right)+2q\psi\left(q^8\right)\right)\left(\varphi^2\left(q^4\right)+4q^2\psi^2\left(q^8\right)\right). \tag{27}$$

Extracting the powers of q that are multiples of 4 and replacing q^4 with q, we get

$$\sum_{n=0}^{\infty} r_{(1,2,2)}(4n)q^n=\varphi^3(q). \tag{28}$$

It follows that if n is even, then

$$r_{(1,2,2)}\left(n^2\right)=r_{(1,1,1)}\left(\frac{n^2}{4}\right)=6\prod_p\left[\frac{p^{\lambda_p+1}-1}{p-1}-\left(\frac{-1}{p}\right)\frac{p^{\lambda_p}-1}{p-1}\right], \tag{29}$$

where the last step follows by Hurwitz's Theorem 1.1.

It remains to determine the value of $r_{(1,2,2)}(n^2)$ when n is odd. If we extract the terms in (27) whose powers of q are congruent to 1 modulo 4 and simplify the resulting identity, we get

$$\sum_{n=0}^{\infty} r_{(1,2,2)}(4n+1)q^n=2\psi\left(q^2\right)\varphi^2(q). \tag{30}$$

On the other hand, we may apply Lemma 4.2 to the result of (28) to get

$$\sum_{n=0}^{\infty} r_{(1,2,2)}(4n)q^n=\varphi^3(q)=\left(\varphi\left(q^4\right)+2q\psi\left(q^8\right)\right)^3.$$

We extract the powers of q that are congruent to 1 modulo 4 and simplify to get

$$\sum_{n=0}^{\infty} r_{(1,2,2)}(16n+4)q^n=6\psi\left(q^2\right)\varphi^2(q). \tag{31}$$

On comparing (30) and (31) we deduce that

$$r_{(1,2,2)}(4n+1)=\frac{1}{3}r_{(1,2,2)}(16n+4). \tag{32}$$

Therefore, if n is odd, by (29) and (32) we deduce that

$$r_{(1,2,2)}\left(n^2\right)=\frac{1}{3}r_{(1,2,2)}\left(4n^2\right)=2\prod_p\left[\frac{p^{\lambda_p+1}-1}{p-1}-\left(\frac{-1}{p}\right)\frac{p^{\lambda_p}-1}{p-1}\right]. \tag{33}$$

The identities (29) and (33) establish the truth of Theorem 1.4. □

7. Proof of Theorem 1.5

The proof of Theorem 1.5 consists of three parts: first we treat the prime 2, then the prime 3, and finally the remaining primes.

We begin with the prime 2. The analogues of Lemmas 4.3 and 4.4 are given by the following two lemmas, respectively.

Lemma 7.1. *The following identities hold*:

$$\varphi(q)\varphi^2\left(q^3\right)\big|_4=\varphi(q)\varphi^2\left(q^3\right)+8q\psi\left(q^2\right)\psi^2\left(q^3\right),$$
$$q\psi\left(q^2\right)\psi^2\left(q^3\right)\big|_4=2q\psi\left(q^2\right)\psi^2\left(q^3\right),$$

and

$$\varphi(q)\varphi^2\left(q^3\right)\big|_{16}=3\varphi(q)\varphi^2\left(q^3\right)\big|_4-2\varphi(q)\varphi^2\left(q^3\right).$$

Lemma 7.2. *The following identities hold*:

$$\sum_{n=0}^{\infty}r_{(1,3,3)}(4n+1)q^n=2\psi\left(q^2\right)\varphi^2\left(q^3\right)$$

and

$$\sum_{n=0}^{\infty}r_{(1,3,3)}(16n+4)q^n=10\psi\left(q^2\right)\varphi^2\left(q^3\right).$$

The proofs of Lemmas 7.1 and 7.2 are very similar to the proofs of Lemmas 4.3 and 4.4, so we omit them. We now fix a positive odd integer m. For any non-negative integer λ, let

$$f(\lambda)=r_{(1,3,3)}\left(2^{2\lambda}m^2\right).$$

By Lemmas 7.1 and 7.2 we deduce that

$$f(\lambda)=3f(\lambda-1)-2f(\lambda-2),\quad \text{provided } \lambda\geqslant 2, \tag{34}$$

and

$$f(1) = 5f(0). \tag{35}$$

The solution of (34) and (35) is given by

$$f(\lambda) = \left(2^{\lambda+2} - 3\right) f(0),$$

and it follows that

$$r_{(1,3,3)}\left(2^{2\lambda} m^2\right) = \left(2^{\lambda+2} - 3\right) r_{(1,3,3)}\left(m^2\right) \tag{36}$$

for any odd positive integer m. This completes the first part of the proof. It remains to determine the value of $r_{(1,3,3)}(m^2)$ for odd values of m.

We will require the following theta function identities.

Lemma 7.3. *Let $X(q)$ and $P(q)$ be defined by*

$$X(q) = \sum_{j=-\infty}^{\infty} q^{3j^2+2j} \quad \text{and} \quad P(q) = \sum_{j=-\infty}^{\infty} q^{j(3j+1)/2}.$$

Then

$$\varphi(q) = \varphi\left(q^9\right) + 2qX\left(q^3\right),$$
$$X(q) = P\left(q^8\right) + qX\left(q^4\right),$$

and

$$\varphi^2(q)P\left(q^2\right) = \varphi^2\left(q^3\right)P\left(q^2\right) + 4q\psi^2\left(q^3\right)X(q).$$

Proof. These are (v), (xviii) and (xxxii), respectively, in [5]. □

The prime $p = 3$ may now be handled as follows. By the first part of Lemma 7.3 we have

$$\varphi(q)\varphi^2\left(q^3\right) = \left(\varphi\left(q^9\right) + 2qX\left(q^3\right)\right)\varphi^2\left(q^3\right). \tag{37}$$

Extracting the terms whose powers are multiples of 3 and then replacing q^3 with q, we get

$$\sum_{n=0}^{\infty} r_{(1,3,3)}(3n)q^n = \varphi\left(q^3\right)\varphi^2(q).$$

Repeating the procedure we get

$$\sum_{n=0}^{\infty} r_{(1,3,3)}(3n)q^n = \varphi\left(q^3\right)\left(\varphi\left(q^9\right) + 2qX\left(q^3\right)\right)^2$$

and so

$$\sum_{n=0}^{\infty} r_{(1,3,3)}(9n)q^n = \varphi(q)\varphi^2(q^3).$$

It follows that $r_{(1,3,3)}(9n) = r_{(1,3,3)}(n)$ and hence

$$r_{(1,3,3)}\left(3^{2\lambda}n^2\right) = r_{(1,3,3)}\left(n^2\right) \tag{38}$$

for any integer n and non-negative integer λ.

By (36) and (38), it remains to determine the value of $r_{(1,3,3)}(n^2)$ in the case that $\gcd(n,6) = 1$. This will be accomplished by the use of

Proposition 7.4. *For any non-negative integer n, we have*

$$r_{(1,3,3)}(12n+1) = \frac{1}{3} r_{(1,1,1)}(12n+1).$$

Proof. If we extract the powers in (37) that are congruent to 1 modulo 3 and simplify, we obtain

$$\sum_{n=0}^{\infty} r_{(1,3,3)}(3n+1)q^n = 2\varphi^2(q)X(q).$$

To this, we apply Lemmas 4.2 and 7.3 and deduce that

$$\sum_{n=0}^{\infty} r_{(1,3,3)}(3n+1)q^n = 2\left(\varphi\left(q^4\right) + 2q\psi\left(q^8\right)\right)^2\left(P\left(q^8\right) + qX\left(q^4\right)\right).$$

Now extract the powers of q that are multiples of 4 and simplify, to get

$$\sum_{n=0}^{\infty} r_{(1,3,3)}(12n+1)q^n = 2\varphi^2(q)P\left(q^2\right). \tag{39}$$

Next, if we cube the first identity in Lemma 7.3, extract the powers of q that are congruent to 1 modulo 3 and simplify, we obtain

$$\sum_{n=0}^{\infty} r_{(1,1,1)}(3n+1)q^n = 6\varphi^2\left(q^3\right)X(q).$$

To this, we apply Lemmas 4.2 and 7.3 and deduce that

$$\sum_{n=0}^{\infty} r_{(1,1,1)}(3n+1)q^n = 6\left(\varphi\left(q^{12}\right) + 2q^3\psi\left(q^{24}\right)\right)^2\left(P\left(q^8\right) + qX\left(q^4\right)\right).$$

Now extract the powers of q that are multiples of 4 and simplify, to get

$$\sum_{n=0}^{\infty} r_{(1,1,1)}(12n+1)q^n = 6\varphi^2\left(q^3\right)P\left(q^2\right) + 24q\varphi\left(q^3\right)\psi\left(q^6\right)X(q).$$

This may be simplified further, by (6) and the last part of Lemma 7.3, to get

$$\sum_{n=0}^{\infty} r_{(1,1,1)}(12n+1)q^n = 6\varphi^2\left(q^3\right)P\left(q^2\right) + 24q\psi^2\left(q^3\right)X(q)$$
$$= 6\varphi^2(q)P\left(q^2\right). \tag{40}$$

On comparing (39) and (40) we complete the proof of Proposition 7.4. □

We are now ready for

Proof of Theorem 1.5. Write the prime factorization of n in the form

$$n = 2^{\lambda_2}3^{\lambda_3}m \quad \text{where } m = \prod_{p\geqslant 5} p^{\lambda_p},$$

and note that since $\gcd(m,6)=1$ we have $m^2 \equiv 1 \pmod{12}$. On successively applying (36), (38) and then Proposition 7.4, we get

$$\begin{aligned} r_{(1,3,3)}\left(n^2\right) &= r_{(1,3,3)}\left(2^{2\lambda_2}3^{2\lambda_3}m^2\right) \\ &= \left(2^{\lambda_2+2}-3\right)r_{(1,3,3)}\left(3^{2\lambda_3}m^2\right) \\ &= \left(2^{\lambda_2+2}-3\right)r_{(1,3,3)}\left(m^2\right) \\ &= \frac{1}{3}\left(2^{\lambda_2+2}-3\right)r_{(1,1,1)}\left(m^2\right). \end{aligned}$$

Hurwitz's Theorem 1.1 may be used to give the value of $r_{(1,1,1)}(m^2)$. This completes the proof of Theorem 1.5. □

8. Conjectures and scope for future work

The results of Theorems 1.1–1.5 suggest there may be similar results for equations of the type

$$n^2 = x^2 + by^2 + cz^2$$

for other positive integers b and c. Without loss of generality, we assume $b \leqslant c$. Based on computer investigations over the domain $1 \leqslant b \leqslant c \leqslant 200$, we have:

Conjecture 8.1. *Let b and c have any of the values given in Table 1. Let n be a positive integer with prime factorization given by (1). The number of $(x,y,z) \in \mathbf{Z}^3$ such that*

$$n^2 = x^2 + by^2 + cz^2$$

is given by a formula of the type

$$r_{(1,b,c)}\left(n^2\right) = \left(\prod_{p\mid 2bc} g(b,c,p,\lambda_p)\right)\left(\prod_{p\nmid 2bc} h(b,c,p,\lambda_p)\right),$$

Table 1
Data for Conjecture 8.1.

b	c
1	1, 2, 3, 4, 5, 6, 8, 9, 12, 21, 24
2	2, 3, 4, 5, 6, 8, 10, 13, 16, 22, 40, 70
3	3, 4, 5, 6, 9, 10, 12, 18, 21, 30, 45
4	4, 6, 8, 12, 24
5	5, 8, 10, 13, 25, 40
6	6, 9, 16, 18, 24
8	8, 10, 13, 16, 40
9	9, 12, 21, 24
10	30
12	12
16	24
21	21
24	24

where

$$h(b,c,p,\lambda_p)=\frac{p^{\lambda_p+1}-1}{p-1}-\left(\frac{-bc}{p}\right)\frac{p^{\lambda_p}-1}{p-1}$$

and $g(b,c,p,\lambda_p)$ has to be determined on an individual and case-by-case basis.

By Theorems 1.1–1.5, Conjecture 8.1 is true for the cases $(b,c)=(1,1)$, $(1,2)$, $(1,3)$, $(2,2)$ and $(3,3)$, respectively.

More detailed conjectures may be formulated in terms of the operator $T_{p^2}(b,c)$, defined for any prime $p\nmid 2bc$ by

$$T_{p^2}(b,c)\left(\sum_{j=0}^{\infty}c_jq^j\right)=\sum_{j=0}^{\infty}c_{p^2j}q^j+\sum_{j=0}^{\infty}\left(\frac{-bcj}{p}\right)c_jq^j+p\sum_{j=0}^{\infty}c_jq^{p^2j},$$

where $(\frac{-bcj}{p})$ is the Legendre symbol. Based on computer investigations, we have:

Conjecture 8.2. *Let b and c have any of the values given in Table 2. Then for any prime p with $p\nmid 2bc$ we have*

$$T_{p^2}(b,c)\big(\varphi(q)\varphi\big(q^b\big)\varphi\big(q^c\big)\big)=(p+1)\varphi(q)\varphi\big(q^b\big)\varphi\big(q^c\big).$$

It is well-known that Conjecture 8.2 is true for the case $(b,c)=(1,1)$, for example, see [9].

Conjecture 8.2 and induction can be used to deduce the factors that involve $h(b,c,p,\lambda_p)$ in Conjecture 8.1. The data in Table 2 is a subset of Table 1.

An example of a case that is covered by Conjecture 8.1 but not by Conjecture 8.2, consider the example $(b,c)=(3,5)$. For this case, we have, for any prime $p\geqslant 7$,

$$\begin{aligned}&T_{p^2}(3,5)\big(\varphi(q)\varphi\big(q^3\big)\varphi\big(q^5\big)\big)\\&\quad=(p+1)\varphi(q)\varphi\big(q^3\big)\varphi\big(q^5\big)+k(p)q^2\prod_{j=1}^{\infty}\frac{(1-q^{2j})^4(1-q^{15j})(1-q^{60j})}{(1-q^j)(1-q^{4j})(1-q^{30j})},\end{aligned}\tag{41}$$

where $k(p)$ is an integer that depends on the prime p. The term that involves the infinite product in (41) has leading coefficient $k(p)q^2$, that is, there is no term that involves q. It follows that induction

Table 2
Data for Conjecture 8.2.

b	c
1	1, 2, 3, 4, 5, 6, 8, 9, 12, 21, 24
2	2, 3, 4, 5, 6, 8, 10, 16
3	3, 4, 6, 9, 10, 12, 18, 30
4	4, 6, 8, 12, 24
5	5, 8, 10, 25, 40
6	6, 9, 16, 18, 24
8	8, 16, 40
9	9, 12, 21, 24
10	30
12	12
16	24
21	21
24	24

can be used to deduce the factors that involve $h(3,5,p,\lambda_p)$ for $p \geqslant 7$ in Conjecture 8.1. The other examples that are in Table 1 but not in Table 2 behave similarly.

References

[1] B.C. Berndt, Ramanujan's Notebooks, Part III, Springer-Verlag, New York, 1991.
[2] B.C. Berndt, Ramanujan's Notebooks, Part V, Springer-Verlag, New York, 1998.
[3] B.C. Berndt, Number Theory in the Spirit of Ramanujan, American Mathematical Society, Providence, RI, 2006.
[4] B. Cho, D. Kim, J.K. Koo, Divisor functions arising from q-series, Publ. Math. Debrecen 76 (2010) 495–508.
[5] S. Cooper, M.D. Hirschhorn, Results of Hurwitz type for three squares, Discrete Math. 274 (2004) 9–24.
[6] S. Cooper, M.D. Hirschhorn, Sums of squares and sums of triangular numbers, Georgian Math. J. 13 (2006) 675–686.
[7] N.J. Fine, Basic Hypergeometric Series and Applications, American Mathematical Society, Providence, RI, 1988.
[8] M.D. Hirschhorn, Partial fractions and four classical theorems of number theory, Amer. Math. Monthly 107 (2000) 260–264.
[9] M.D. Hirschhorn, J.A. Sellers, On representations of a number as a sum of three squares, Discrete Math. 199 (1999) 85–101.
[10] A. Hurwitz, Sur la décomposition des nombres en cinq carrés, C. R. Acad. Sci. 98 (1884) 504–507.
[11] A. Hurwitz, L'Intermédiaire des Mathematiciens 14 (1907) 107.
[12] C.D. Olds, On the representations, $N_3(n^2)$, Bull. Amer. Math. Soc. 47 (1941) 499–503.
[13] S. Ramanujan, Notebooks, Tata Institute of Fundamental Research, Bombay, 1957 (2 vols.).
[14] H.F. Sandham, A square as the sum of 7 squares, Quart. J. Math. (2) 4 (1953) 230–236.
[15] Z.H. Sun, My conjectures in number theory, http://www.hytc.edu.cn/xsjl/szh/mycon.pdf, 2011.
[16] K.S. Williams, Number Theory in the Spirit of Liouville, Cambridge University Press, Cambridge, 2010.